[19]中华人民共和国国家知识产权局

[51]Int.Cl⁷
H04L 9/32

[12]发明专利申请公开说明书

[21]申请号 99123276.3

[43]公开日 2000年5月17日

[11]公开号 CN 1253438A

[22]申请日 1999.10.29 [21]申请号 99123276.3

[30]优先权

[32]1998.10.30 [33]JP [31]309806/1998

[71]申请人 株式会社日立制作所

地址 日本东京

[72]发明人 土山千佳子 丰岛久 永井康彦

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

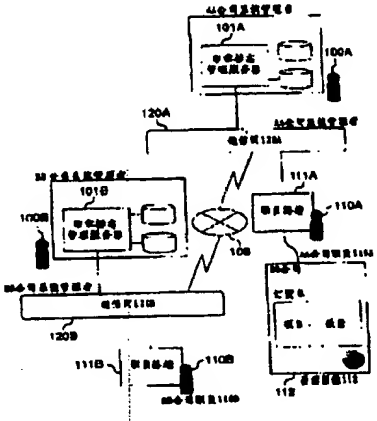
代理人 范本国

权利要求书 4 页 说明书 18 页 附图页数 13 页

[54]发明名称 数字署名或电子印章认证系统及认证标志管理程序

[57]摘要

本发明为一种利用用于提供可以实现在网上收发数字数据时的本人认证和数据 认证的技术的数字标志进行数字数据的认证的标志管理服务器。该服务器具有一个标志管理处理部分和一个标志译码键管理处理部分。标志管理处理部分接 收新登录或更新标志登录要求,作成嵌入到该要求端的标志图案中的标志并将 译码键添加到上述作成的标志中配置到要求端。标志译码键管理处理部分将译 码键登录到标志译码键管理数据库中并向各标志终端装置发送。



ISSN1008-4274

权 利 要 求 书

1. 一种用于提供可用于通过数字标志来对数据进行认证的标志的数字标志认证系统，其特征在于：具有根据作成标志的要求为了作成在显示器上有识别性的标志而将用户的认证信息嵌入到用户的标志图案中的标志管理处理部分（221）；和将用于将上述标志进行译码的译码键和上述识别性标志配置到用户终端装置上的标志配置部分（200—222）。

2. 如权利要求1所述的数字标志认证系统，其特征在于：具有存储上述译码键的译码键管理数据库和将上述译码键向与上述标志管理服务器连接的多个标志终端装置发送的译码键处理部分（222）。

3. 如权利要求1或2所述的数字标志认证系统，其特征在于：在显示器上用眼睛确认上述认证信息嵌入到上述作成的标志中的情况。

4. 如权利要求1、2或3所述的数字标志认证系统，其特征在于：上述认证信息通过用密码键将包含用户的特征的信息进行加密而得到。

5. 如权利要求1、2、3或4所述的数字标志认证系统，其特征在于：根据更新标志的要求，上述标志管理处理部分（221）为了作成用户的其他认证信息而用密码键将包含用户的其他特征的信息进行加密，为了作成上述标志而将上述其他认证信息嵌入到用户的标志图案中。

6. 如权利要求1、2、3、4或5所述的数字标志认证系统，其特征在于：根据作成上述标志的要求，标志管理处理部分（221）为了作成用户的认证信息，将不能在显示器上用眼睛确认将其他认证信息嵌入到包含用户的其他特征而作成的上述标志中的情况的上述其他认证信息嵌入到标志图案中。

7. 如权利要求6所述的数字标志认证系统，其特征在于：上述

认证信息和上述其他认证信息嵌入到上述标志中分割的不同的场所.

8. 一种将用于通过数字标志来对数据进行认证的标志附加到数字数据上的终端装置，其特征在于：具有将用于作成标志的要求向数字标志认证系统发送并从该系统接收用密码键将包含用户本人的特征的信息进行加密从而将上述认证信息嵌入到用户的标志图案中的标志并进行存储的标志处理部分（312）、用于接收并存储将上述标志译码的译码键的译码键数据库（315）和为了认证应发送的数字数据而用上述密码键将上述数字数据的登录信息进行加密并嵌入到上述标志中与上述数字数据一起发送的发送部分（303）.

9. 一种电子印章认证系统，其特征在于：至少 1 个委托终端与管理在上述委托终端中使用的标志的至少 1 个管理服务器通过通信网相互连接，上述标志管理服务器具有在从上述委托终端接收到标志的登录或变更要求时将为了进行数字数据的作成者的本人认证所需要的信息嵌入到标志中并向上述委托终端发送的单元，上述委托终端具有将为了进行数字数据的文书认证所需要的信息宛如到标志中的单元和进行数字数据的本人认证和文书认证中的任意一种或两种的单元.

10. 如权利要求 9 所述的电子印章认证系统，其特征在于：在发行标志时将为了进行本人认证所需要的信息供给 1 个图像图形数据内的 1 个块，在发送文书时将为了进行文书认证所需要的信息供给不同的块，生成具有进行本人认证和文书认证中的任意一种或两种的单元的具有识别性的印章标志.

11. 一种用于提供用于通过数字标志来对数据进行认证的标志的数字标志认证方法，其特征在于：包括根据作成标志的要求为了作成在显示器上有识别性的标志而将用户的认证信息嵌入到用户的标志图案中的步骤（1008）和将用于将上述标志进行译码的译码键和上述识别性标志配置到用户终端装置上的步骤（1010）.

12. 如权利要求 11 所述的数字标志认证方法，其特征在于：包

括从存储上述译码键的译码键管理数据库将上述译码键向与上述标志管理服务器连接的多个标志终端装置发送的步骤（1010）.

13. 如权利要求 11 或 12 所述的数字标志认证方法，其特征在于：在显示器上用眼睛确认上述认证信息嵌入到上述作成的标志中的情况。

14. 如权利要求 11、12 或 13 所述的数字标志认证方法，其特征在于：包括为了得到上述认证信息而用密码键将包含用户的特征的信息进行加密的步骤。

15. 如权利要求 11、12、13 或 14 所述的数字标志认证方法，其特征在于：包括根据更新标志的要求，为了作成用户的其他认证信息而用密码键将包含用户的其他特征的信息进行加密、为了作成上述标志而将上述其他认证信息嵌入到用户的标志图案中的步骤.

16. 如权利要求 11、12、13、14 或 15 所述的数字标志认证方法，其特征在于：包括根据作成上述标志的要求，为了作成用户的认证信息将不能在显示器上用眼睛确认将其他认证信息嵌入到包含用户的其他特征而作成的上述标志中的情况的上述其他认证信息嵌入到标志图案中的步骤.

17. 如权利要求 16 所述的数字标志认证方法，其特征在于：将上述认证信息和上述其他认证信息嵌入到上述标志中分割的不同的场所.

18. 一种使将用于通过数字标志来对数据进行认证的标志附加到数字数据中的终端装置操作的方法，其特征在于：包括将用于作成标志的要求向数字标志认证系统发送，从该系统接收并存储将上述认证信息嵌入到用密码键将包含用户本人的特征的信息进行加密的用户的标志图案中的步骤（1011）、接收并存储用于将上述标志译码的译码键的步骤（1012）和为了认证应发送的数字数据用上述密码键将上述数字数据的登录信息进行加密并嵌入到上述标志中与上述数字数据一起发送的步骤（1116）.

19. 一种用于提供用于通过数字标志来对数据进行认证的标志

的数字标志认证程序，其特征在于：包括根据作成标志的要求为了作成在显示器上有识别性的标志而将用户的认证信息嵌入到用户的标志图案中的步骤（1008）和将用于将上述标志进行译码的译码键和上述识别性标志配置到用户终端装置上的步骤（1010）.

20. 一种在将用于通过数字标志来对数据进行认证的标志附加到数字数据中的终端装置上运行的程序，其特征在于：包括将用于作成标志的要求向数字标志认证系统发送，从该系统接收并存储将上述认证信息嵌入到用密码键将包含用户本人的特征的信息进行加密的用户的标志图案中的步骤（1011）、接收并存储用于将上述标志译码的译码键的步骤（1012）和为了认证应发送的数字数据用上述密码键将上述数字数据的登录信息进行加密并嵌入到上述标志中与上述数字数据一起发送的步骤（1116）.

说　　明　　书

数字署名或电子印章认证系统及认证标志管理程序

本发明涉及利用电子标志来对数字数据进行认证的数字标志认证系统，特别涉及适用于利用表示图章印痕及署名的数字标志来对数字数据进行认证的数字标志认证系统的有效技术.

JP－A－10－11509号说明书公开了一种资料保安系统.

在网上的商务交易等广泛开展的现在，可以在网上确认所传输的信息的可靠性的技术就变得非常重要。对于确认是否完全没有被第 3 者冒充的本人认证，有利用护照或信用卡等持有物的方式、利用指纹、声迹或笔迹等生物统计学的方式和利用口令或数字署名等秘密信息的方式等。但是，在网上使用时，通常是使用持有物或秘密信息的方式。

另外，对于在传输信息的过程中的中途涂改的确认，在利用因特网的电子商务（EC，Electronic Commerce）中为安全地进行信用卡结账而使用的 SET（Secure Electronic Transactions）中，是用数字署名来进行持卡人的认证的。数字署名就是用发送装置的密码键将通常想传输的信息压缩后的压缩文进行加密的密码文，可以用发送装置的译码键（公开键）译码为原来的压缩文。即，接收者通过将根据所接收的信息作成的压缩文与根据接收的数字署名所译码的压缩文进行比较，便可进行信息是否进行了涂改的确认，即可以进行文书认证。

文书等的数字数据的接收者仅看了该数字数据是不能确认信息的正当性和发送者的。在现实社会中，有时根据看了印在纸上的印章的图样就可以确认，具有安心感。但是，可以说数字署名还不具有给人这样的安心感的识别性。

另一方面，以往的电子印章系统中使用了人眼看了就可以确认

的图章印痕，但是，图章印痕本身仅仅是一种图案，文书等数字数据的接收者为了确认发送者，必须检查登录信息等的历史等情况。

本发明的目的就是要解决上述问题，提供一种在网上收发数字数据时可以实现本人认证或数据认证的技术。

本发明的另一目的在于提供一种可以对包含用人眼可以确认的标志的发送信息进行认证的技术。

本发明是一种用于提供用于通过数字标志来对数据进行认证的标志的数字标志认证系统，其特征在于包括：根据作成标志的要求为了作成在显示器上有识别性的标志而将用户的认证信息嵌入到用户的标志图案中的标志管理处理部分（221）；和将用于把上述标志进行译码的译码键和上述识别性标志配置到用户终端装置上的标志配置部分（200—222）。

在显示器上用人眼可以确认认证信息嵌入到该作成的标志中这一情况。通过用密码键将包含用户的特征的信息进行加密，便可得到认证信息。

根据标志更新要求，上述标志管理处理部分（221）为了作成用户的其他认证信息而用密码键将包含用户的其他特征的信息进行加密，为了作成上述标志，可以将上述其他认证信息嵌入到用户的标志图案中。

此外，本发明还提供了一种将用于通过数字标志来对数据进行认证的标志附加到数字数据上的终端装置，其特征在于：具有将用于作成标志的要求向数字标志认证系统发送并从该系统接收用密码键将包含用户本人的特征的信息进行加密从而将上述认证信息嵌入到用户的标志图案中的标志并进行存储的标志处理部分（312）；

用于接收并存储将上述标志译码的译码键的译码键数据库（315）；和

为了认证应发送的数字数据而用上述密码键将上述数字数据的登录信息进行加密并嵌入到上述标志中与上述数字数据一起发送的发送部分（303）。

此外，本发明还提供了一种利用数字标志来对数据进行认证的认证系统，其特征在于包括：根据用于作成标志的要求为了作成在显示器上有识别性的标志而将用户的认证信息嵌入到用户的标志图案中的标志管理处理部分（221）；

提供用于将上述标志译码的译码键和上述识别性标志的标志管理部分（200—222）；和

为了对应发送的数字数据进行认证而用上述密码键将上述数字数据的登录信息进行加密并嵌入到上述标志中与上述数字数据一起进行发送的发送部分（303）.

在利用表示图章印痕或署名的标志进行数字数据的认证的电子标志认证系统的标志认证处理部分中，可以把将本人认证信息和数字数据认证信息嵌入到标志图案中的标志附加到数字数据上，使用标志中的认证信息进行该数字数据的认证。

本发明的标志终端装置的标志登录处理部分将电子印章等的标志的新登录或要求更新的标志登录要求向标志管理服务器发送时，标志管理服务器的标志管理处理部分就接收标志登录要求，将用密码键将用于认证要求端的人物的信息进行加密的本人认证信息嵌入到该要求端的图章印痕图案等的标志图案中，作成标志，将用于对上述本人认证信息进行译码的译码键添加到上述行程的标志中，配置到要求端。

另外，标志管理服务器的标志译码键管理处理部分将用于对上述密码化的本人认证信息进行译码的译码键登录到标志译码键管理数据库中，将上述登录的译码键向各标志终端装置发送。

标志终端装置的标志登录处理部分接收从标志管理服务器的标志管理处理部分发送来的标志，各标志终端装置的译码键存储处理部分接收从标志译码键管理处理部分发送来的译码键并存储到译码键数据库中.

标志终端装置的标志附加处理部分对附加了标志的文书等数字数据用用户固有的密码键将包含其特征信息的数字数据认证信息和

标志附加通配符进行加密，将上述密码化的数字数据认证信息和标志附加通配符嵌入到已嵌入了发送该数字数据的用户的本人认证信息的标志中，将上述标志附加到选择上述数字数据的位置。

如上所述，附加了标志的数字数据向其他用户的标志终端装置发送时，该标志终端装置的标志认证处理部分就从附加在数字数据中的标志中抽出本人认证信息，将为了对该本人认证信息进行译码而添加的译码键与存储在译码键数据库中的译码键进行对照，判断它们是否一致，在上述译码键一致时，就用上述译码键对从上述标志中抽出的本人认证信息进行译码，并显示本人认证信息，在上述译码键不一致时，就显示错误信息。

另外，标志终端装置的标志认证处理部分从附加在数字数据中的标志中抽出数字数据认证信息，利用译码键进行译码，从附加了标志的数字数据中抽出特征信息，并将从上述数字数据中抽出的特征信息与从标志中抽出的数字数据认证信息中的特征信息进行比较对照，在特征信息一致时，就显示上述数字数据认证信息，在特征信息不一致时，就显示错误信息。

如上所述，按照本发明的电子标志认证系统，将嵌入本人认证信息和数字数据认证信息而作成的标志附加到数字数据中，使用标志中的认证信息进行该数字数据的认证，所以，可以在确保以数据的发送者为象征的识别性的基础上实现在网上收发数字数据时的本人认证和数据认证。

图 1 是表示本实施例的电子印章认证系统的概略结构图。

图 2 是表示本实施例的印章标志管理服务器 101 的概略结构图。

图 3 是表示本实施例的职员终端 111 的概略结构图。

图 4 是表示本实施例的印章标志管理数据库 210 的数据例的示意图。

图 5 是表示本实施例的印章标志公开键管理数据库 211 的数据例的示意图。

图 6 是表示本实施例的本人认证数据的示例图，

图 7 是表示本实施例的文书认证数据的示例图.

图 8 是表示本实施例的图章印痕和印章标志的图形例的示意图.

图 9 是表示本实施例的初始画面的图形例的示意图.

图 10 是表示本实施例的印章标志登录处理的处理顺序的流程图.

图 11 是表示本实施例的印章标志按压处理的处理顺序的流程图.

图 12 是表示本实施例的与图 11 的处理流程对应的处理画面的示意图.

图 13 是表示本实施例的本人认证处理的处理顺序的流程图.

图 14 是表示本实施例的与图 13 的处理流程对应的处理画面的示意图.

图 15 是表示本实施例的文书认证处理的处理顺序的流程图.

图 16 是表示本实施例的与图 15 的处理流程对应的处理画面的示意图.

下面详细说明在企业内部网和企业间网络中使用数字署名或印章进行本人认证和文书认证的一个实施例的电子标志认证系统.

图 1 是表示本实施例的数字标志认证系统的概略结构图. 本实施例的电子标志认证系统是管理印章标志或署名标志的多个系统管理者 100A ~ 100B（以下，也简称为系统管理者 100）和多个职员 110A ~ 110B（以下，也简称为职员 110）利用的系统，如图 1 所示，由标志管理服务器 101A（以下，也简称为标志管理服务器 101）和职员终端 111A（以下，也简称为职员终端 111）通过企业内部网等通信网 120A（以下，也简称为通信网 120）相互连接而构成. BB 公司的同样的系统或客户终端通过因特网 108 等与其连接.

这里所说的标志，是指包含表示有识别性的本人的象征的要素的图像数据，表示用于进行对于按压印章或进行署名的本人是否完

全没有被第 3 者冒充的验证（以下，也简称为本人认证）和按压了印章或署名的文书等的数字数据是否没有被涂改的验证（以下，也简称为文书认证）所采用的图形图案的形状的印章或署名的标志。该图形图案可以比一般字符的编码信息冗长。

标志管理服务器 101 在系统管理者 100 管理的企业内部网及企业之间的网络中进行本人认证和文书认证。标志管理服务器 101 根据职员 110 的要求将标志作为对各自的本人认证所需要的信息登录到后面所述的标志管理数据库中。这时，标志的图案可以由职员 110 可以用扫描器使实际的图章印痕及人的头像照片等数字化的方法等自由地作成。但是，为了防止不正当的登录，要通过职员 ID 等进行该作成者的确认。

职员 110 使用职员终端 111 作成商务所需要的文书等，或者与系统管理者 100 之间进行数据的收发。各自的标志由职员终端 111 等进行管理。在作成者要求变更所属的包含在印章或署名中的信息时，系统管理者 100 就进行标志的更新，并将更新后的标志向职员终端 111 发送。画面图形 112 是显示带印章标志的数字数据时的画面显示例。

图 2 是表示本实施例的标志管理服务器 101 的概略结构图。图 2 所示的本实施例的标志管理服务器 101 具有标志管理处理部分 221 和标志公开键管理处理部分 222。

标志管理处理部分 221 通过通信网 120A 从职员终端 111 接收新登录或要求更新的标志登录要求，利用后面所述的电子水印技术将用密码键使用于认证要求端的人物的信息进行加密的本人认证信息嵌入到该要求端的图章印痕或署名图案中，作成标志并将用于对上述本人认证信息进行译码的公开键添加到上述作成的标志中从而配置到要求端。

标志公开键管理处理部分 222 是将用于对密码化的本人认证信息进行译码的公开键登录到标志公开键管理数据库 211 中并将上述登录的公开键向各职员终端 111 发送的标志公开或译码键管理处理

部分.

用于使标志管理服务器 101 实现标志管理处理部分 221 和标志公开键管理处理部分 222 的功能的程序记录到 CD—ROM 等记录媒体上并存储到磁盘等中后，装载到存储器中来执行. 记录上述程序的媒体，也可以是 CD—ROM 以外的其他媒体.

图 2 所示的本实施例的标志管理服务器 101 由显示装置 201、输入装置 202、通信网接口 203、标志管理数据库接口 204、标志公开键管理数据库接口 205、标志登录管理数据库接口 206、存储装置 207、CPU208 和存储器 209 通过总线 200 相互连接而构成. 另外，作为外部存储装置，还连接着标志管理数据库 210、标志公开键管理数据库 211 和标志登录管理数据库 212.

显示装置 201 用于向使用标志管理服务器 101 的系统管理者 100 显示信息等，由 CRT 或液晶显示器等构成. 输入装置 202 用于供使用标志管理服务器 101 的系统管理者 100 输入数据及命令等，由键盘或鼠标器等构成. 通信网接口 203 是通过通信网 120 用于进行职员终端 111 与其他公司的标志管理服务器 101B 等进行数据收发的接口.

标志管理数据库接口 204 是用于与标志管理数据库 210 进行数据收发的接口. 标志管理数据库 210 使职员 ID、印章／署名 ID、图章印痕／署名等这样的数据彼此对应而进行管理，例如图 4 所示的那样.

标志公开键管理数据库接口 205 是用于与标志公开键管理数据库 211 进行数据的收发的接口. 标志数据库 211 使有交易的企业的信息系统管理部分等的标志管理者和本人认证用的公开键等这样的数据彼此对应而进行管理，例如图 5 所示的那样.

标志登录管理数据库接口 206 是用于与标志登录管理数据库 212 进行数据的收发的接口. 标志登录管理数据库 212 在按压标志／进行署名时使嵌入到该标志中的文书认证数据与数字数据彼此对应而进行管理，例如图 7 所示的那样.

存储装置 207 是为了永远连续地存储在标志管理服务器 101 等中使用的程序及数据而使用的，由硬盘或软盘等构成。

CPU208 统一地控制构成标志管理服务器 101 的各部分，进行各种各样的运算处理。存储器 209 用于暂时存储称为 OS220 及标志管理处理部分 221 和标志公开键管理处理部分 222 的 CPU208 进行上述处理所需要的程序等。

这里，OS220 是为了进行印章标志管理服务器 101 全体的控制而实现称为文件管理及过程管理或设备管理的功能的程序。

标志管理处理部分 221 是进行在从职员终端 111 有标志登录/变更要求时确认是否为第 3 者的不正当的要求的处理、在判定为进行登录时将本人信息嵌入到发送来的署名或图章印痕图案或者由标志管理数据库 210 管理的图案中的处理、根据上述处理而更新标志管理数据库 210 的处理、将标志向要求端发送的处理和将发送来的登录信息存储到标志登录管理数据库 212 中的处理的处理部分。

另外，标志管理数据库 210 只有有权限的人才可以更新。嵌入到图案中的本人信息是图 6 所示的那样的信息。将特定的信息嵌入到图像数据中的技术，众所周知的就是“电子水印”技术，有不能用人眼进行判其他嵌入信息的不可见水印和以人眼可以看见的形式嵌入信息的可见水印。在不可见水印的情况时，嵌入的信息量是有限的，但是，为了防止不正当的行为，有效的情况还是不少的。只要是在知道标志的图形所象征的意义的范围内，即只要是在知道该标志表示什么内容的范围内，即使多少改变图案也不会有什么影响，所以，可以如图 8 所示的那样将可见水印和不可见水印组合，嵌入更多的信息。

标志公开键管理处理部分 222 进行为了确认按压到公司外的数字文书上的标志的发送者即进行本人认证而将所需要的公开键登录到标志公开键管理数据库 211 中并进行管理的处理、以及如果新的公开键登录到了标志公开键管理数据库 211 中就将该公开键向与职员终端 111 等连接的公开键数据库发送的处理和在有要求发送公开

键时就将该公开键向要求端发送的处理。

从公司外接收到公开键时，企业的系统管理者 100 为了防止被第 3 者冒充，在进行了发送端的身份确认后，还要接收在软盘（FD）等中存储的公开键。

图 3 是表示本实施例的职员终端 111 的概略结构图。图 3 所示的本实施例的职员终端 111 具有标志登录处理部分 312、标志按压处理部分 313、标志认证处理部分 314 和公开键存储处理部分 315。

标志登录处理部分 312 是向标志管理服务器 101 发送要求标志的新登录或更新的标志登录要求并从标志管理服务器 101 中接收将用密码键使用于认证要求端的人物的信息进行加密的本人认证信息嵌入到该要求端的图案而作成的标志的标志登录处理部分。

标志按压处理部分 313 是用用户固有的密码键使包含附加了标志的文书的特征信息的文书认证信息和通配符进行加密并将上述密码化的文书认证信息和通配符嵌入到已嵌入了本人认证信息的标志中从而将上述标志附加到上述文书所选择的强制的标志附加处理部分。

标志认证处理部分 314 进行从附加到文书中的标志中抽出本人认证信息、将为了对该本人认证信息进行译码而添加的公开键与公开键数据库 309 存储的公开键对照是否一致并在上述公开键一致时就用上述公开键对从上述标志中抽出的本人认证信息进行译码并显示本人认证信息而在上述公开键不一致时就显示错误信息的本人认证处理；和从附加到文书中的标志中抽出文书认证信息并利用公开键进行译码、从附加了标志的文书中抽出特征信息、将从上述文书中抽出的特征信息与从标志中抽出的文书认证信息中的特征信息进行比较对照并在特征信息一致时就显示上述文书特征信息而在特征信息不一致时就显示错误信息的数据认证处理。公开键存储处理部分 315 是从标志管理服务器 101 中接收用于将本人认证信息译码的公开键并将上述公开键存储到公开键数据库 309 中的译码键存储处理部分。

用于使职员终端 111 实现标志登录处理部分 312、标志按压处理部分 313、标志认证处理部分 314 和公开键存储处理部分 315 的功能的程序记录到 CD—ROM 等记录媒体并存储到磁盘等上后，装载到存储器中来执行．记录上述程序的媒体也可以是 CD—ROM 以外的其他媒体．

如图 3 所示，本实施例的职员终端 111 由显示装置 301、输入装置 302、通信网接口 303、公开键 D 接口 304、存储装置 305、CPU306 和存储器 307 通过总线 300 相互连接而构成．以往，在利用在公司内使用的图案时，在用位图等读入连接图像扫描器 308 而使用的图案后，可以进行编辑．

显示装置 301 是为了向使用职员终端 111 的职员显示信息等而使用的，由 CRT 或液晶显示器等构成．输入装置 302 用于供使用职员终端 111 的职员 110 输入数据或命令等，由键盘或鼠标等构成．通信网接口 303 是用于标志管理服务器 101 与职员终端 111B 等通过通信网 120 进行收发数据的接口．

公开键数据库接口 304 是在有公开键数据库 309 时用于进行收发数据的接口．存储装置 305 用于永远连续地存储在职员终端 111 等中使用的程序及数据而使用的，由硬盘或软盘等构成。

CPU306 统一地控制构成职员终端 111 的各部分，进行各种各样的运算处理．存储器 307 中暂时存储称为 OS310 和分组系统等 311、标志认证处理部分 314、标志信息存储部分 316 的 CPU306 为了进行上述处理所需要的程序等．

这里，OS310 是为了进行职员终端 111 全体的控制而用于实现称为文件管理及过程管理或设备管理的功能的程序．分组系统等 311 是职员终端 111 与公司内外收发数字数据用于显示所需要的数据的系统，为了处理附加到数字数据中的认证信息，具有与标志认证处理部分 314 的接口．只要该分组系统等 311 的部分是处理数字数据的应用系统，不论是什么的都可以，对分组系统并没有特别限定．另外，有时也可以直接将标志认证处理部分 314 个别地作为应用系

统在 OS310 上使用.

标志登录处理部分 312 进行作成标志登录用的图案的处理、向标志管理服务器 101 发送标志登录要求的处理和接收从标志管理服务器 101 发送来的标志的处理.

标志按压处理部分313进行用于职员 110 用职员终端 111 对数字数据进行数字署名或签名或按压印章的处理、如果显示了所需要的数字数据并输入了与职员 ID 对应的口令就调出与该职员 ID 对应的标志的处理、将用固有的密码键使所选择的文书认证信息和标志的按压通配符等的署名/按压时的信息进行加密的信息嵌入到标志的特定的块中的处理和将标志按压到文书的指定的位置的处理等.

标志认证处理部分314是用于进行职员 110 用职员终端 111 接收的数字数据的发送者及其内容的认证的处理部分. 进行显示所需要的数字数据并与所选择的认证项目对应地使用由标志管理服务器 101 预先配置的公开键将嵌入到标志中的本人认证信息译码并进行显示的本人认证处理、使用添加到标志中的公开键将嵌入到标志中的文书认证信息译码并进行显示的文书认证处理、在不能用上述公开键进行译码时就显示错误信息的处理和检查所显示的数字数据的有效期限及文件名等信息并在判定为无效时就将上述图案变形为无效的图案的处理.

标志信息存储部分 316 是暂时存储由标志认证处理部分 314 使用职员终端 111 调出的标志和公开键的存储部分.

在企业间进行网上交易等为了确认本人认证信息而需要多个公开键时，就将公开键数据库 309 与职员终端 111 或通信网 120 连接，从标志公开键管理数据库 211 向公开键数据库接口 304 发送所需要的公开键数据库 211，可以根据职员终端 111 进行参考. 另外，仅在企业网络内使用标志时，可以预先使职员终端 111 具有公开键，而不限定公开键的存储方法.

图 4 是表示本实施例的标志管理数据库 210 的数据的示例图. 根据一定的标记基准将标记统一，存储职员 ID401、ID402、姓名

403、信箱地址 404、所属·职务等信息 405、图章印痕数据 406 等. 登录新的标志或变更已有的标志的所属·职务等信息 405 时，更新标志管理数据库 210.

图 5 是表示本实施例的标志公开键管理数据库 211 的数据的示例图. 根据一定的标记基准将标记统一，存储数据序号 501、标志管理者 502、管理者地址 503、公开键数据 504 等. 标志公开键管理数据库 211 是管理用于本人认证的公开键数据 504 的数据库，新增加利用标志的企业或变更公开键数据 504 时，就更新标志公开键管理数据库 211. 在预先设定了公开键数据 504 的有效期限等时，也管理该数据.

图 6 是表示本实施例的本人认证数据的示例图. 在图 6 中，表示的是在标志管理服务器 101 中标志管理处理部分 221 根据职员 110 的要求将本人认证信息嵌入到图章印痕中时的本人认证数据的例子.

由标志管理服务器 101 的标志管理处理部分 221 使用由标志管理服务器 101 管理的密码键使职员 ID601、姓名 602、信箱地址 603、所属·职务等 604 进行加密，作为标志的实体而嵌入. 在嵌入时，例如，如图 8 的图章印痕图像 802 那样，对图章印痕的姓名部分以不可见水印的形式嵌入，将公司名以可见水印的形式嵌入. 即，预先将图章印痕中分为 2 个以上的块，将本人认证信息嵌入特定的块中. 在公司图章那样的印章中，有时也将署名／盖章的责任部门作为本人认证信息使用.

图 7 是表示本实施例的文书认证数据的一个例子. 在图 7 中，表示的是在职员终端 111 中职员 110 将标志按压到数字数据上时作为文书认证信息而嵌入的文书认证数据的例子.

职员终端 111 的标志处理部分 313 利用标志处理部分 313 管理的密码键在职员终端 111 中使职员 ID701、标志按压通配符序号 702、作成日期 703、有效期限 704、文件名 705、终端 ID706、按压的数字数据的特征信息 707 等进行加密，作为标志的实体而嵌入. 例如，

如图 8 的图章印痕图像 803 那样，将文书认证信息嵌入到已嵌入了本人认证信息的块以外的图章印痕的周边部分.

作为数字数据的特征信息 707，使用将文字数据的代码视为数值而进行相加的称为所谓的检验和的数据以及数字数据的内容的压缩文等.

另外，图 7 也是标志登录管理数据库 212 的数据例，由职员终端 111 的标志按压处理部分 313 将图 7 所示那样的数据作为署名/盖章的登录信息向标志管理服务器 101 发送，由印章标志管理处理部分 221 将该登录信息存储到标志登录管理数据库 212 中.

本人认证和文书认证所需要的数据不限于图 6 和图 7 的例子，作为取得 ISO9001 的认证时的电子数据的记录信息，也可以视为满足所需要的信息的数据.

图 8 是表示本实施例的图章印痕和标志图像的示例图. 将本人认证信息嵌入到例如图章印痕图像 801 那样的图章印痕中. 这时，预先将图章印痕中分为 2 个以上的块，分别将本人认证信息和文书认证信息嵌入到特定的块中.

例如，分为如图章印痕图像 802 那样将本人认证信息嵌入到姓名部分和可见水印的公司名部分而将文书认证信息嵌入到图章印痕 803 牛的图章印痕的周边部分的这样的块，在由职员终端 111 的标志认证处理部分 314 将认证信息译码时，就自动地从对应的块中提取所嵌入的信息.

在图章印痕图像 801 中，作为图章印痕图案的例子，使用的是个人的图章的图案，但是，也可以使用带日期的行业图章或签名等图案. 另外，作为公司图章使用时，也可以是企业名等，并不限定图章印痕图像 801 的图章印痕图案例. 但是，重要的是与单纯的图像图案不同，嵌入了认证信息时，就是给人一种感到可信赖的图章印痕图案.

下面，说明本实施例的电子认证系统的操作. 图 9 是表示本实施例的初始画面的示意图. 在图 9 中，表示的是由职员终端 111 显

示的电子认证系统的初始画面图像例.

初始画面 900 由显示所需要的数字文书等的数字数据显示区域 901、排列着标志的功能图标的标志功能显示区域 902 和排列着确认、取消、文件这样的基本功能的图标的基本功能显示区域 903 构成。但是，初始画面 900 是各区域的配置并不限定上述配置.

图 10 是表示本实施例的标志登录处理的处理顺序的流程图. 在图 10 中，表示的是在职员终端 111 与标志管理服务器 101 之间进行标志的登录的处理流程.

首先，职员 110 单击图 9 所示的初始画面 900 的标志功能显示区域 902 的登录按钮时，标志登录处理部分 312 就将标志的登录要求向标志管理服务器 101 发送（1001）.

接收到标志登录要求的标志管理服务器 101 就利用标志管理处理部分 221 根据登录要求端的职员 ID401 从标志管理数据库 210 中读出要求端的信箱地址 404，并将标志要求／变更的确认委托向要求端的信箱地址 404 发送（1002 和 1003）.

接收到确认委托的职员终端 111 的标志登录处理部分 312 将使用图像扫描器等作成的登录或想变更的图章印痕图案与标志的要求确认结果一起向标志管理服务器 101 发送（1004 和 1005）. 也可以使用数码相机或数字目录作成软件来取代扫描器作成图章印痕或署名的图案.

接收到图章印痕和标志的要求确认结果的标志管理服务器 101 使用标志管理处理部分 221，用标志管理服务器 101 管理的该服务器的密码键将本人认证信息进行加密，并将其嵌入到所接收的图章印痕图案中，作成标志（1008）.

将标志管理数据库 210 内的登录或变更过的标志的信息更新后（1009），将上述作成的标志与用于对其本人认证信息进行译码的公开键一起使用 FD 等配置给要求端的职员 110（1010）. 职员 110 将配置的标志存储到职员终端 111 中（1011 和 1012）.

图 11 是表示本实施例的标志按压处理的处理顺序的流程图. 在

图 11 中，表示的是在职员终端 111 中将嵌入文书认证信息的标志按印到文书中的处理流程. 图 12 是表示本实施例的与图 11 的处理流程对应的处理画面的示意图. 下面，使用图 11 和图 12 以及上述图 9 说明上述处理流程.

首先，职员 110 利用位于基本功能显示区域 903 中的文件按钮选择想按印的文书数据等并在数字数据显示区域 901 中进行显示（1101）.

单击了标志功能显示区域 902 的标志的调用按钮时，就由标志按印处理部分 313 显示图 12 的处理画面图像 1201 的职员 ID401 和口令的输入栏（1102 和 1103）.

标志按印处理部分 313 将输入的口令与预先存储在职员终端 111 中的口令进行对照，在它们不一致时就显示错误信息，一致时就在标志栏中显示标志（1104 和 1106）.

其次，单击了文书信息的嵌入按钮时，如图 12 的处理画面图像 1202 那样，由标志按印处理部分 313 显示文书认证信息的项目栏（1107 和 1108）.

选择所需要的项目并单击了确认按钮时，标志按印处理部分 313 就用对各职员预先决定的各职员所固有的密码键将所选择的文书信息和通配符进行加密，并嵌入到标志中，另外，添加上译码所需要的公开键，并在标志栏中显示该标志（1109～1113）.

选择了按印位置并单击了标志功能显示区域 902 的按印按钮时，标志按印处理部分 313 就将标志按印到文书的设定的位置（1114～1116）. 在按印后，就可以发送图中所示的定货单. 但是，这里也可以不按印到文书上，而单独发送嵌入了信息的标志. 用于文书认证信息的译码所需要的职员固有的公开键也可以不添加到标志中而在进行本人认证时取得.

图 13 是表示本实施例的本人认证处理的处理顺序的流程图. 图 14 是表示本实施例的与图 13 的处理流程对应的处理画面的示意图. 首先，在职员终端 111 中如图 14 的处理画面图像 1401 那样显

示附加了标志的数字数据，职员 110 单击了标志的认证按钮时，标志认证处理部分 314 就显示标志的认证项目栏（1301 和 1302）.

如图 14 的处理画面图像 1402 那样，职员 110 单击了标志的本人认证项目按钮时，标志认证处理部分 314 就从该标志中提取本人认证信息（1303）. 对照用于将抽出的本人认证信息译码的公开键与存储在职员终端 111 或公开键数据库 309 中的公开键是否一致（1305）.

与用于进行译码的公开键一致时，标志认证处理部分 314 就将从标志中提取出的本人认证信息译码，为了可以确认内容，如图 14 的处理画面图像 1403 那样显示本人认证信息（1306），如果不一致就显示错误信息（1307）. 此外，在显示错误信息时，就进行将图章印痕消除或给图章印痕打上 × 等，将标志变形为无效的图案（1308）.

另外，在本人想确认作为本人认证信息而显示的内容时，就将确认委托的信箱向本人认证信息中的信箱地址发送. 本人认证结果的显示方法并不限定图 14 的处理画面例，例如，也可以利用声音等表现错误信息.

图 15 是表示本实施例的文书认证处理的处理顺序的流程图. 在文书认证处理流程的最初的工序中，省略了与本人认证处理流程相同的部分和与图 13 中的步骤 1301 及 1302 相当的部分. 图 16 是表示本实施例的与图 15 的处理流程对应的处理画面的示意图.

首先，职员 110 如图 16 的处理画面图像 1601 那样在职员终端 111 中单击标志的文书认证项目按钮（1501）. 标志认证处理部分 314 从该标志中抽出文书信息的译码所需要的公开键和文书认证信息，并将文书认证信息译码（1502～1504）.

其次，从按印了该标志的文书等的数字数据中抽出特征信息，与从该标志中抽出的文书认证信息中的特征信息 707 进行比较对照（1505 和 1506）.

结果，不一致时，文书等的数字数据就与作成时刻的不同，所

以，就显示“该数据已变更”等错误信息，并且将图章印痕消除或给图章印痕打上×等，将标志变形为无效的图案（1507和1508）.

特征信息707一致时，就进而确认有效期限等信息，如果被确认，就如图16的处理画面图像1602那样显示确认所需要的文书信息（1509和1510），在有效期限704已超过时，就将图章印痕消除或给图章印痕打上×等，将标志变形为无效的图案（1508）. 文书认证结果的显示方法并不限定图16的处理画面图像例，也可以利用（比方说）声音等表示错误信息.

为了防止标志被第3者不正当的按印，使用了口令，但是，为了进一步提高安全性，可以例如使用ID卡管理口令，在使用时由标志认证处理部分314从ID卡中读出口令. 这时，如果预先将口令进行加密，安全性就更高了.

另外，作为不正当地得到只嵌入了本人认证信息的其他人的标志并用自己的密码键将文书信息嵌入到该标志中而不正当地使用等的对策，可以利用例如标志的按印通配符序号702. 在职员终端111中按印嵌入了文书认证信息的标志时，就将按印通配符序号702作为登录经历信息自动地向标志管理服务器101发送，通过由标志登录管理数据库212管理登录信息，在进行上述不正当的使用时就可以进行检查.

以上，使用企业网络和企业间网络的例子说明了本发明的实施例，但是，本发明不限于该实施例. 例如，也可以适用于个人在网上进行电子商务时作成的定货单那样的在网上进行收发的一般的数字数据. 另外，以往发行印章证明的自治体成为标志管理机关，在进行实际印章的印章登录时，对于申请标志的人，也可以考虑配置嵌入本人认证信息的标志和标志认证处理部分314. 数字数据也不限定文书，也可以是地图等图像数据或活动图像数据.

此外，也可以向管理者终端或数据库发送嵌入了出席或投票用的署名数据的标志.

如上所述，按照本实施例的电子标志认证系统，将嵌入本人认

证信息和数字数据认证信息而作成的标志附加到数字数据中，使用标志中的认证信息进行该数字数据的认证，所以，可以实现在网上收发数字数据时的本人认证和数据认证.

说 明 书 附 图

图1

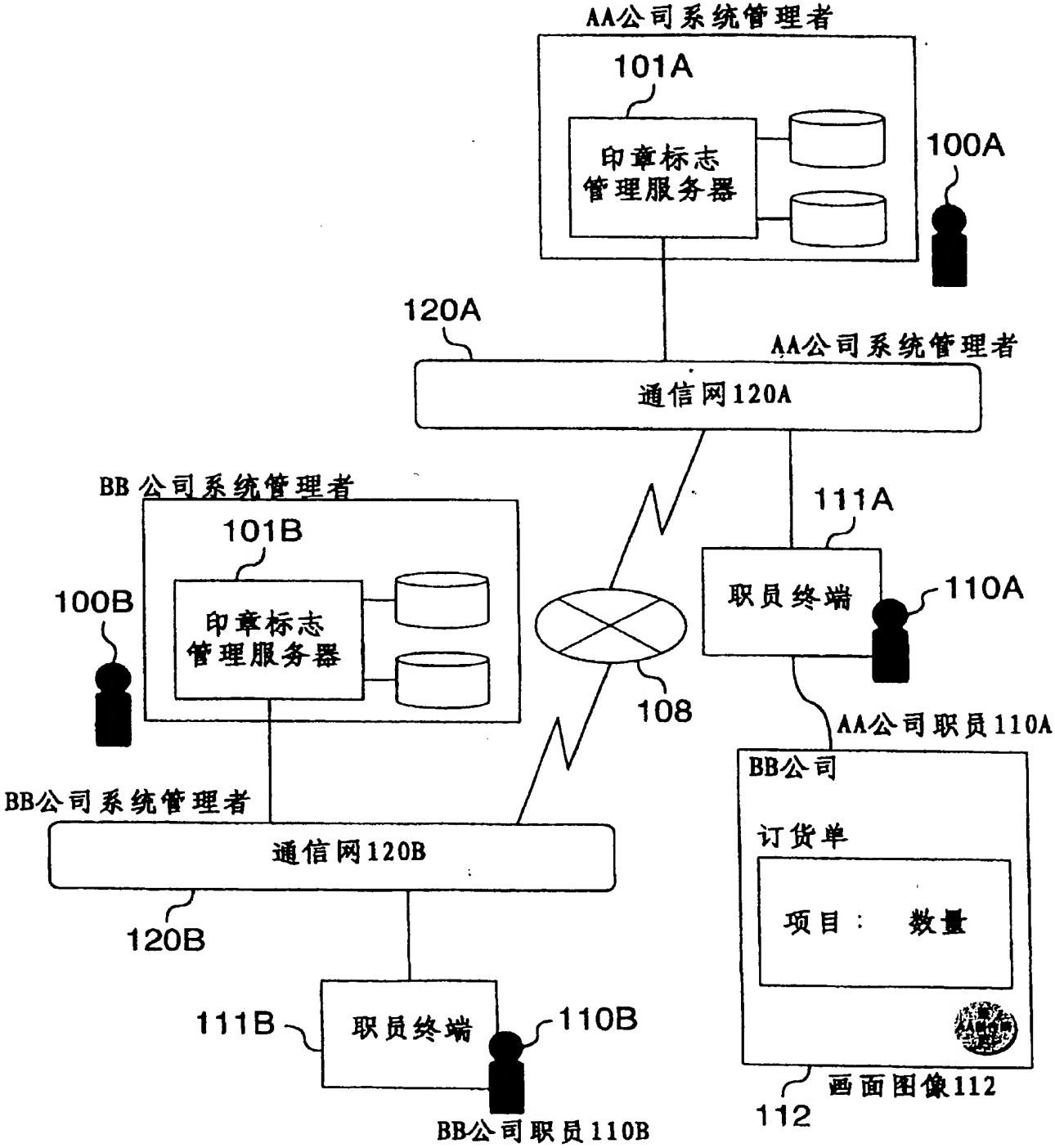

AA公司系统管理者
101A
印章标志
管理服务器
100A
120A
AA公司系统管理者
通信网120A
BB 公司系统管理者
101B
100B
印章标志
管理服务器
111A
职员终端
110A
108
AA公司职员110A
BB公司
订货单
项目： 数量
BB公司系统管理者
通信网120B
120B
111B
职员终端
110B
BB公司职员110B
画面图像112
112

图 2

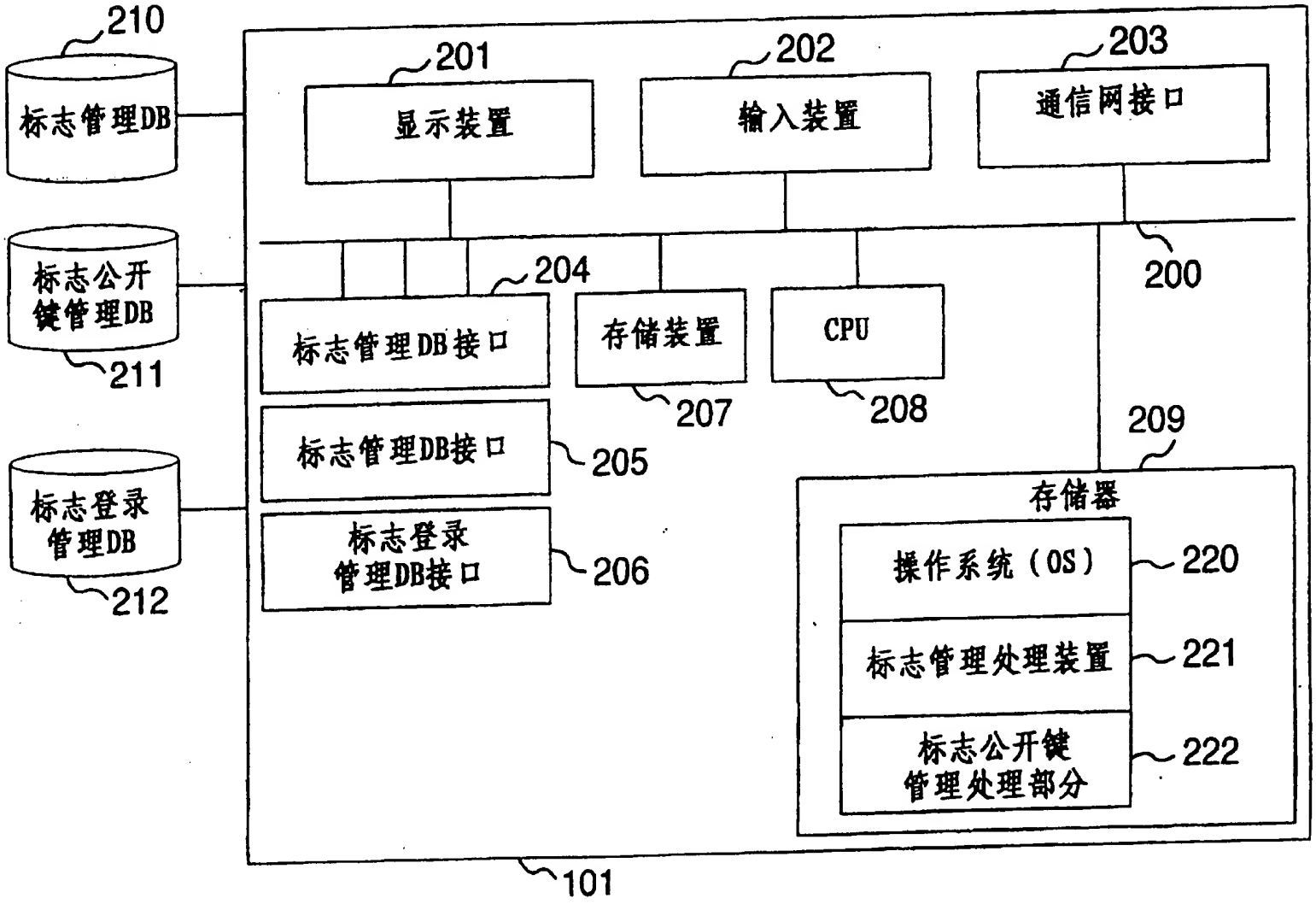

210
标志管理DB
201
显示装置
202
输入装置
203
通信网接口
标志公开
键管理DB
211
204
标志管理DB接口
存储装置
207
CPU
208
200
209
标志管理DB接口
205
存储器
标志登录
管理DB
212
标志登录
管理DB接口
206
操作系统（OS）
220
标志管理处理装置
221
标志公开键
管理处理部分
222
101

图 3

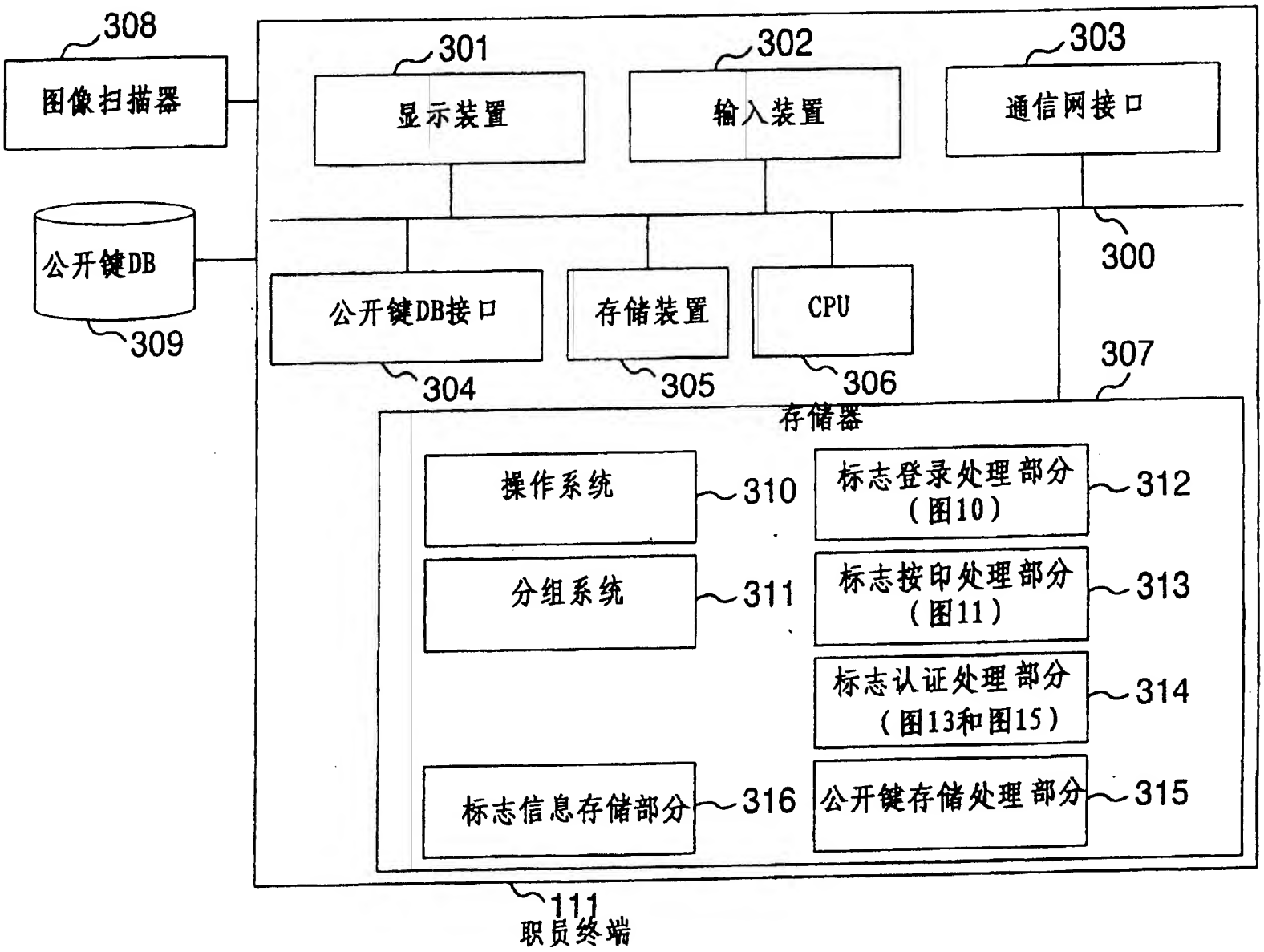

308
图像扫描器
301
显示装置
302
输入装置
303
通信网接口
公开键DB
309
300
公开键DB接口
304
存储装置
305
CPU
306
307
存储器
操作系统
310
标志登录处理部分
（图10）
312
分组系统
311
标志按印处理部分
（图11）
313
标志认证处理部分
（图13和图15）
314
标志信息存储部分
316
公开键存储处理部分
315
111
职员终端

图 4

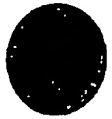
401 职员ID	402 文章ID	403 姓名	404 信箱地址	405 所属．职务等	406 图章印痕
D001101117	A00123	相川太郎	Aikawa@aa.co.jp	○○事业部 事业部长	
A035410506	A00124	藍田次郎	Aida@aa.co.jp	○○事业部 课长	
H001100402	-	爱野三郎	Aino@aa.co.jp	○○事业部 担当	-

图5

501 NO.	502 印章标志管理者	503 管理者地址	504 公开键
1	A公司印章标志管理	im@aa.co.jp	pw****gl*****qqm*
2	B公司印章标志管理	im@bb.co.jp	*ajk**yu*****aqz*r

图6

601 印章ID	602 姓名	603 信箱地址	604 所属。职务等
A00123	相川太郎	Aikawa@aa.co.jp	○○事业部 事业部分

图7

701 印章ID	702 通配符序号	703 作成日期	704 有效期限	705 文件名	706 终端ID	707 数据的特征信息
A00123	000089	1998.7.7	1998.12.31	158.2**/**.doc	PC792	********

图8

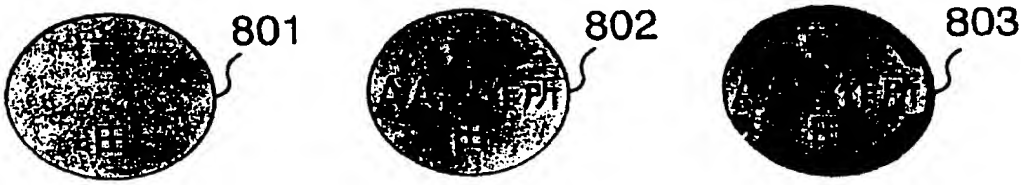


图9

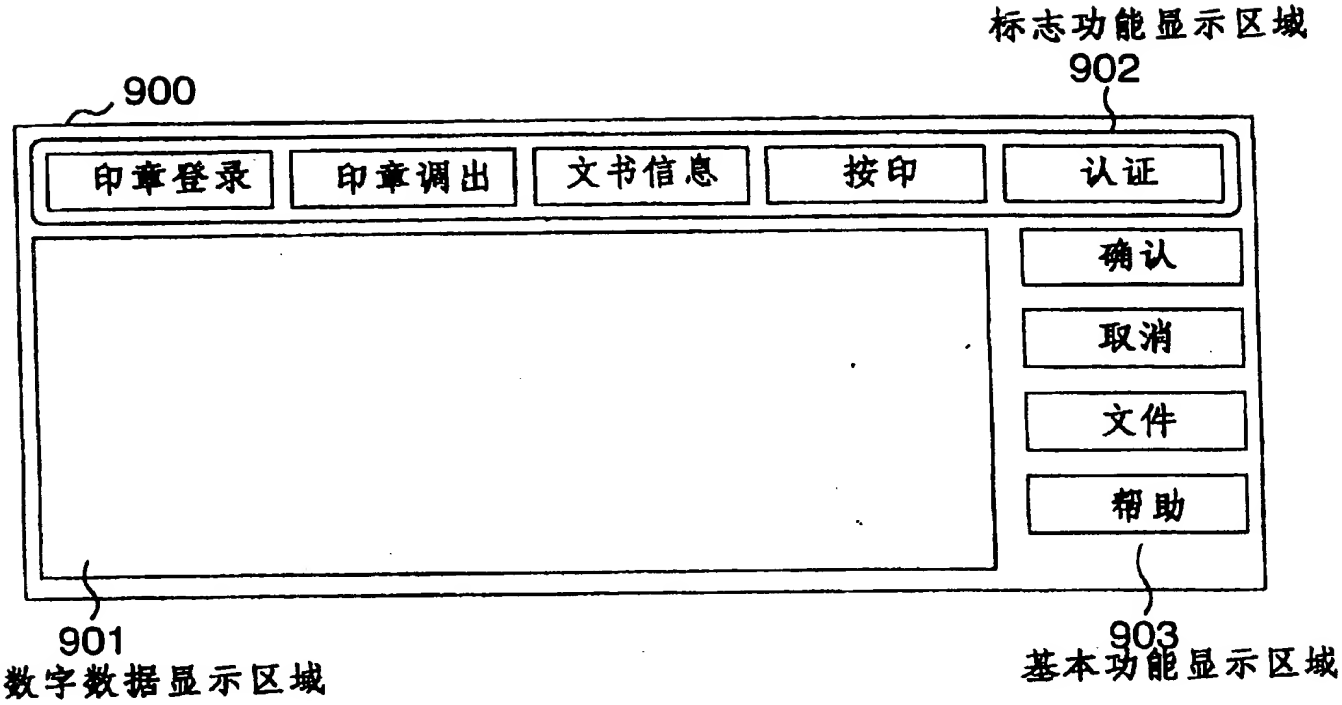

标志功能显示区域
902
900
印章登录
印章调出
文书信息
按印
认证
确认
取消
文件
帮助
901
数字数据显示区域
903
基本功能显示区域

图10

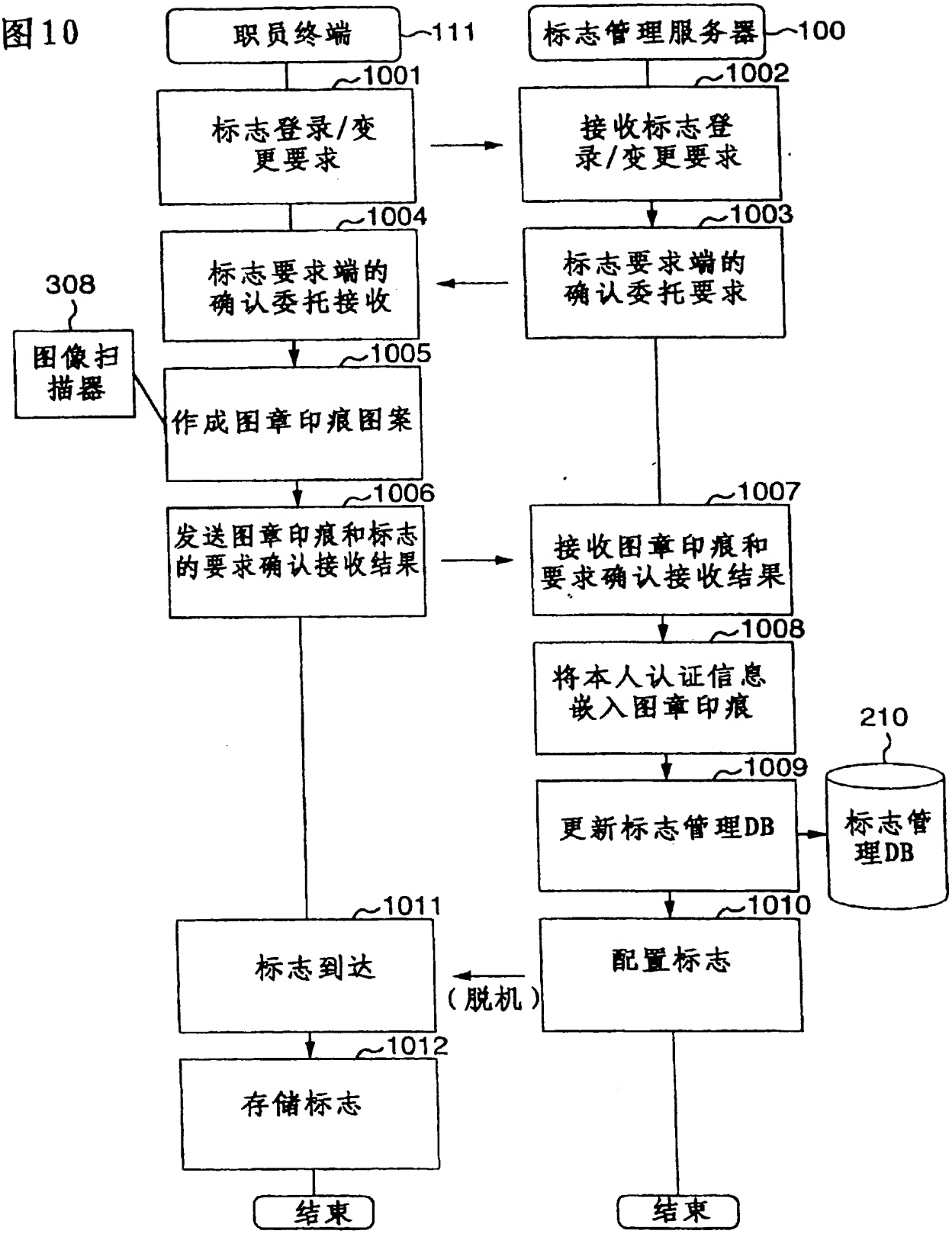

职员终端
111
标志管理服务器
100
1001
标志登录/变更要求
1002
接收标志登录/变更要求
1004
标志要求端的确认委托接收
1003
标志要求端的确认委托要求
308
图像扫描器
1005
作成图章印痕图案
1006
发送图章印痕和标志的要求确认接收结果
1007
接收图章印痕和要求确认接收结果
1008
将本人认证信息嵌入图章印痕
210
1009
更新标志管理DB
标志管理DB
1011
标志到达
(脱机)
1010
配置标志
1012
存储标志
结束
结束

图11

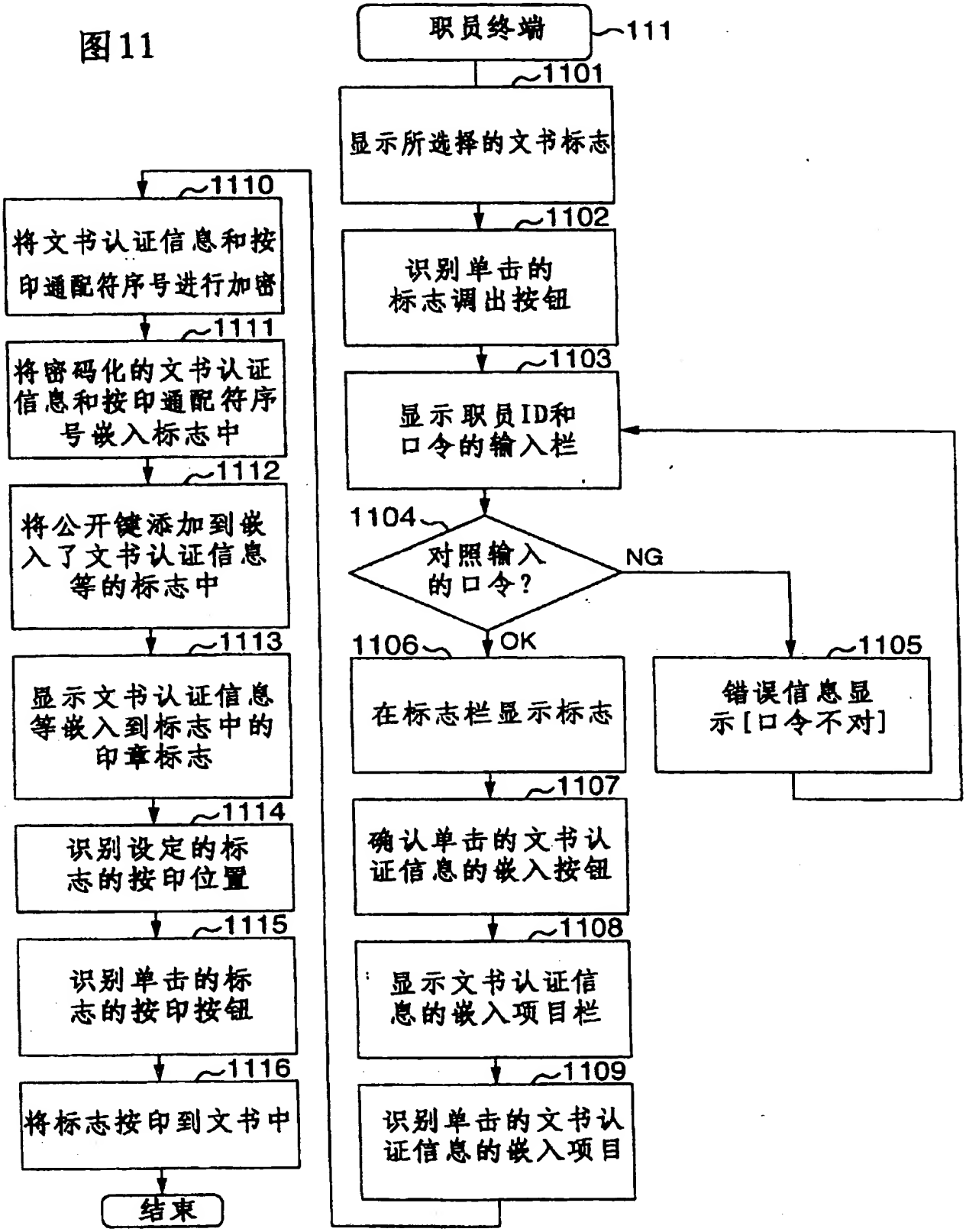

职员终端
111
1101
显示所选择的文书标志
1102
识别单击的标志调出按钮
1103
显示职员ID和口令的输入栏
1104
对照输入的口令？
NG
OK
1105
错误信息显示[口令不对]
1106
在标志栏显示标志
1107
确认单击的文书认证信息的嵌入按钮
1108
显示文书认证信息的嵌入项目栏
1109
识别单击的文书认证信息的嵌入项目
1110
将文书认证信息和按印通配符序号进行加密
1111
将密码化的文书认证信息和按印通配符序号嵌入标志中
1112
将公开键添加到嵌入了文书认证信息等的标志中
1113
显示文书认证信息等嵌入到标志中的印章标志
1114
识别设定的标志的按印位置
1115
识别单击的标志的按印按钮
1116
将标志按印到文书中
结束

图12

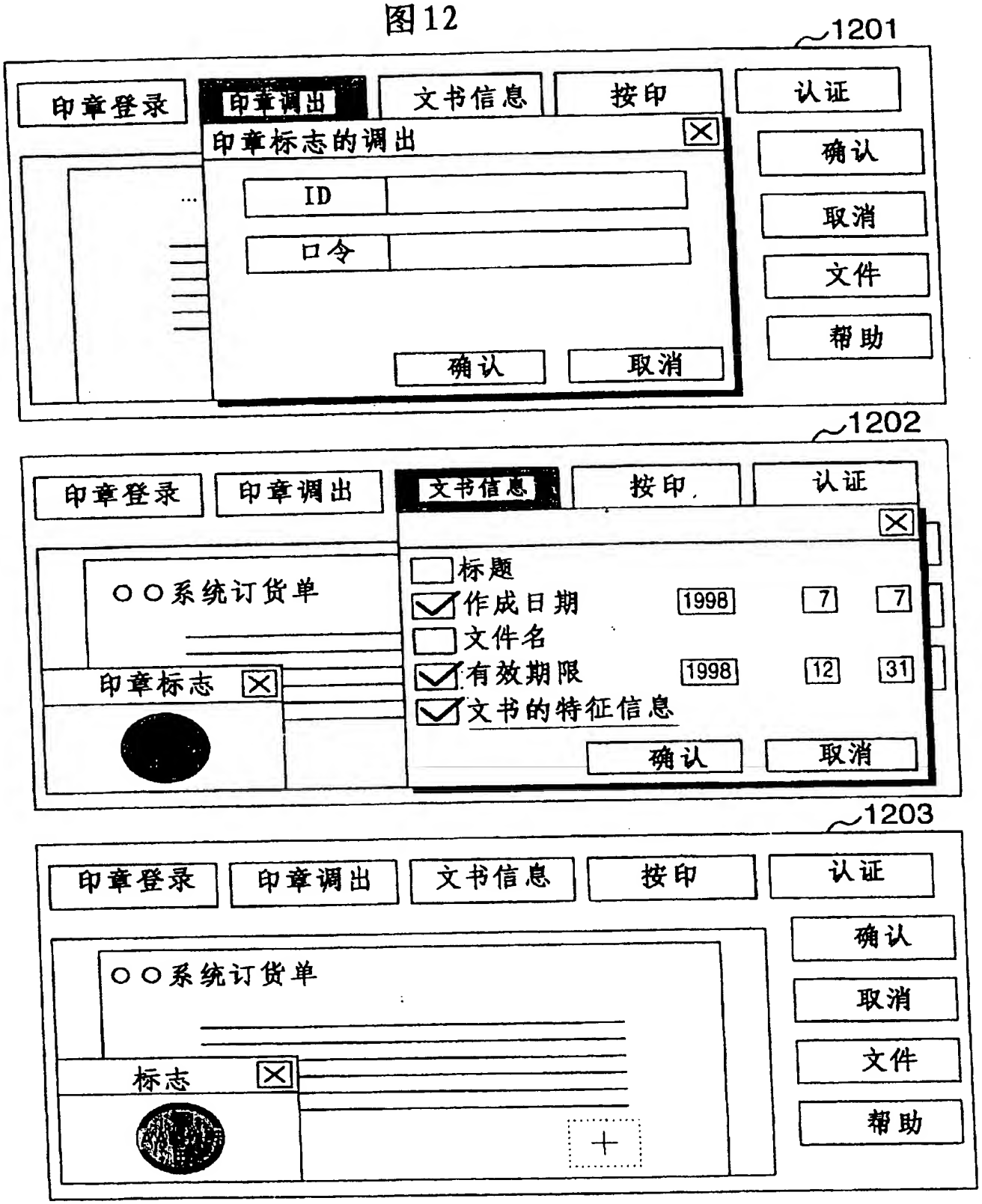

1201
印章登录
印章调出
文书信息
按印
认证
印章标志的调出
ID
口令
确认
取消
确认
取消
文件
帮助
1202
印章登录
印章调出
文书信息
按印
认证
○○系统订货单
印章标志
标题
作成日期
1998
7
7
文件名
有效期限
1998
12
31
文书的特征信息
确认
取消
1203
印章登录
印章调出
文书信息
按印
认证
○○系统订货单
标志
确认
取消
文件
帮助

图13

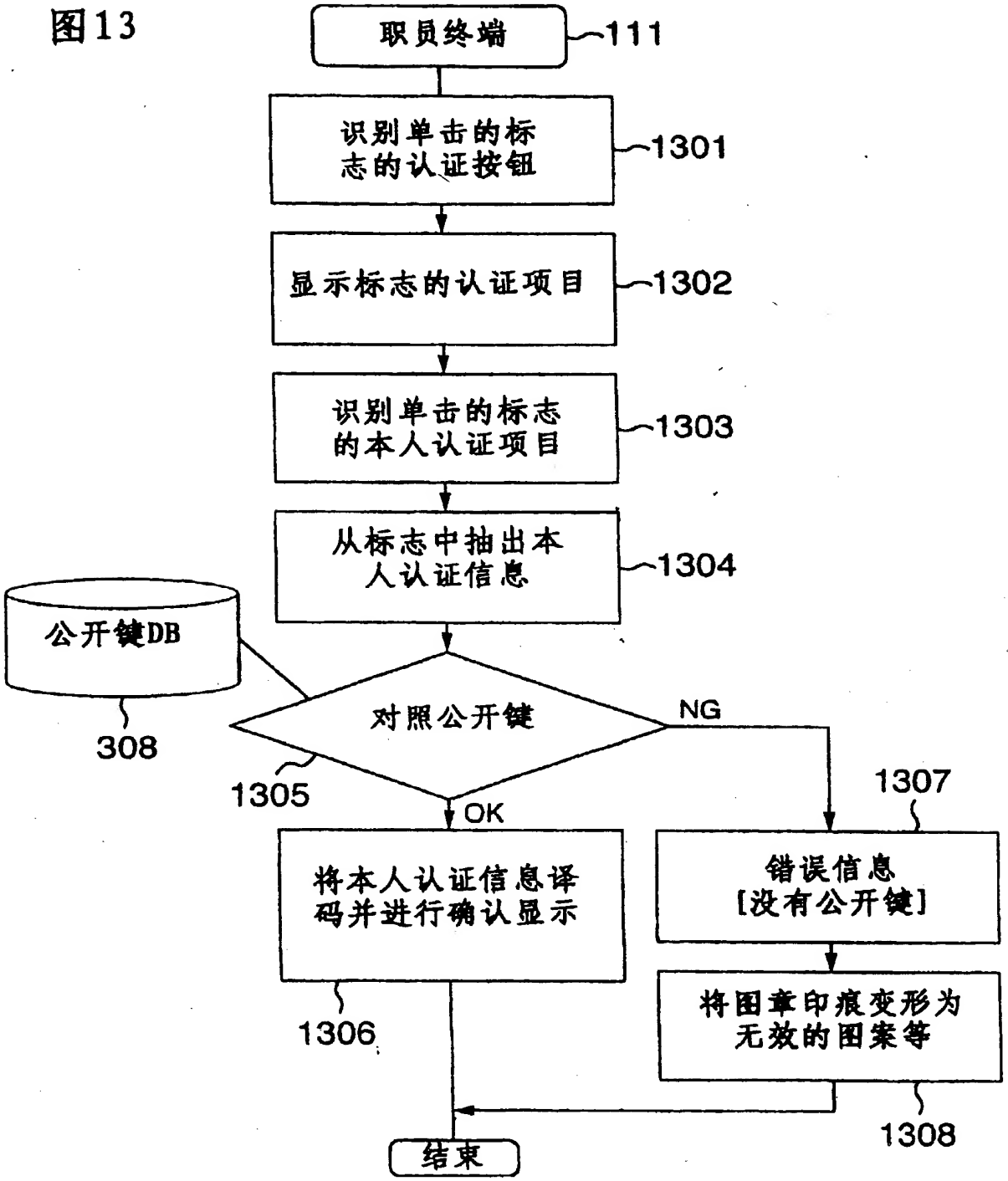

职员终端
111
识别单击的标志的认证按钮
1301
显示标志的认证项目
1302
识别单击的标志的本人认证项目
1303
从标志中抽出本人认证信息
1304
公开键DB
308
对照公开键
1305
NG
OK
1307
将本人认证信息译码并进行确认显示
1306
错误信息[没有公开键]
将图章印痕变形为无效的图案等
1308
结束

图14

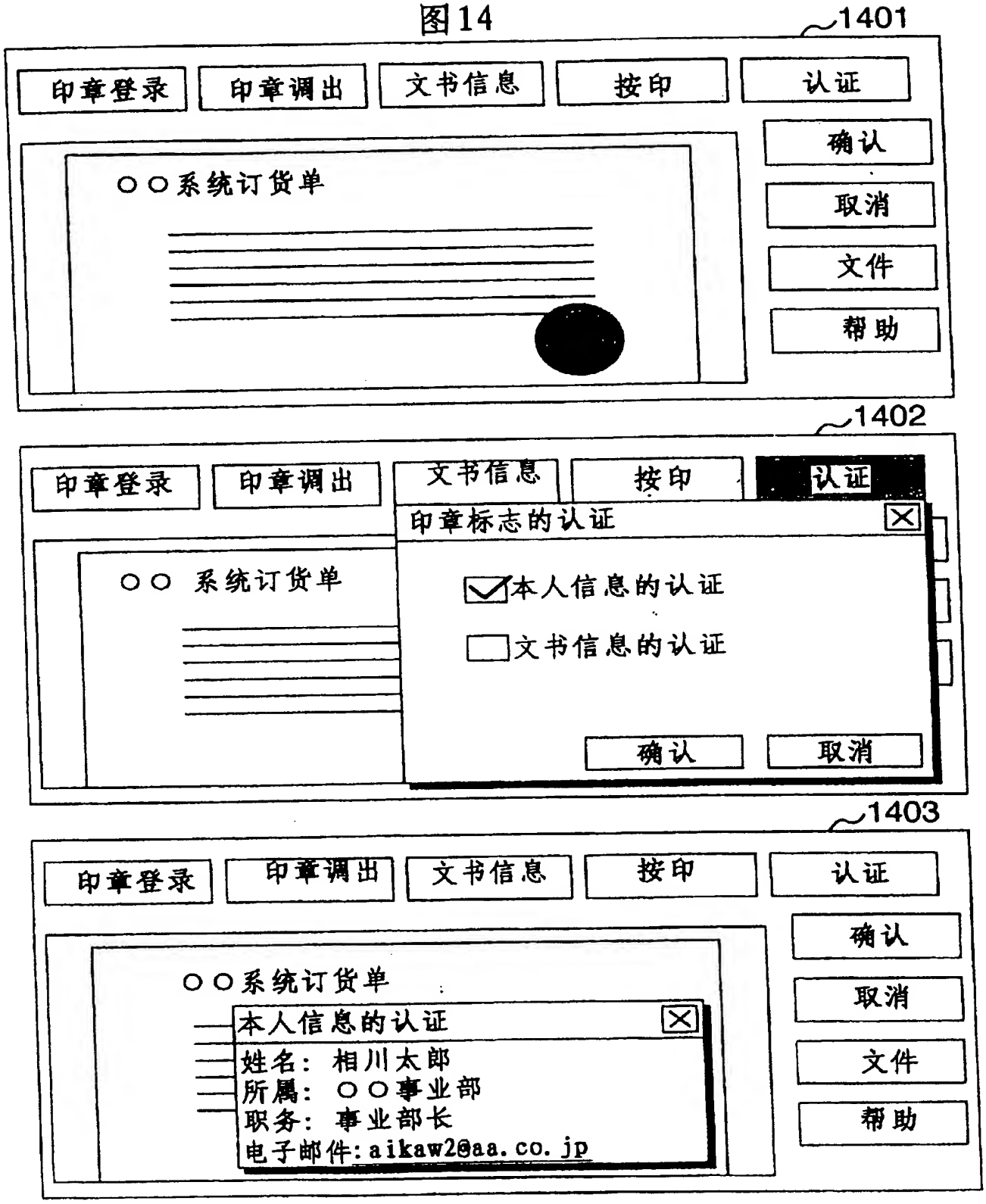

1401
印章登录
印章调出
文书信息
按印
认证
确认
取消
文件
帮助
○○系统订货单
1402
印章登录
印章调出
文书信息
按印
认证
印章标志的认证
○○ 系统订货单
本人信息的认证
文书信息的认证
确认
取消
1403
印章登录
印章调出
文书信息
按印
认证
确认
取消
文件
帮助
○○系统订货单
本人信息的认证
姓名：相川太郎
所属：○○事业部
职务：事业部长
电子邮件：aikaw2@aa.co.jp

图15

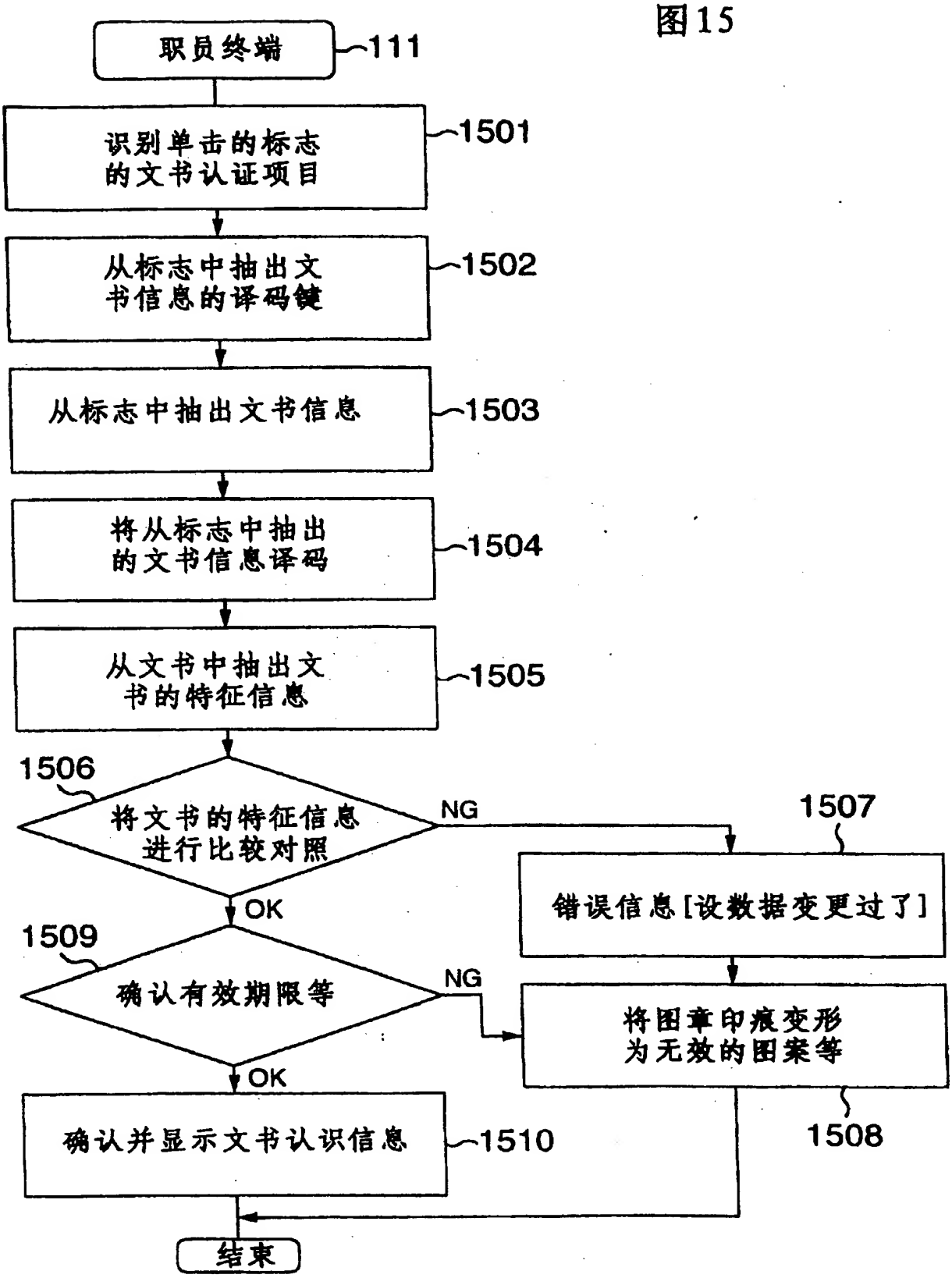
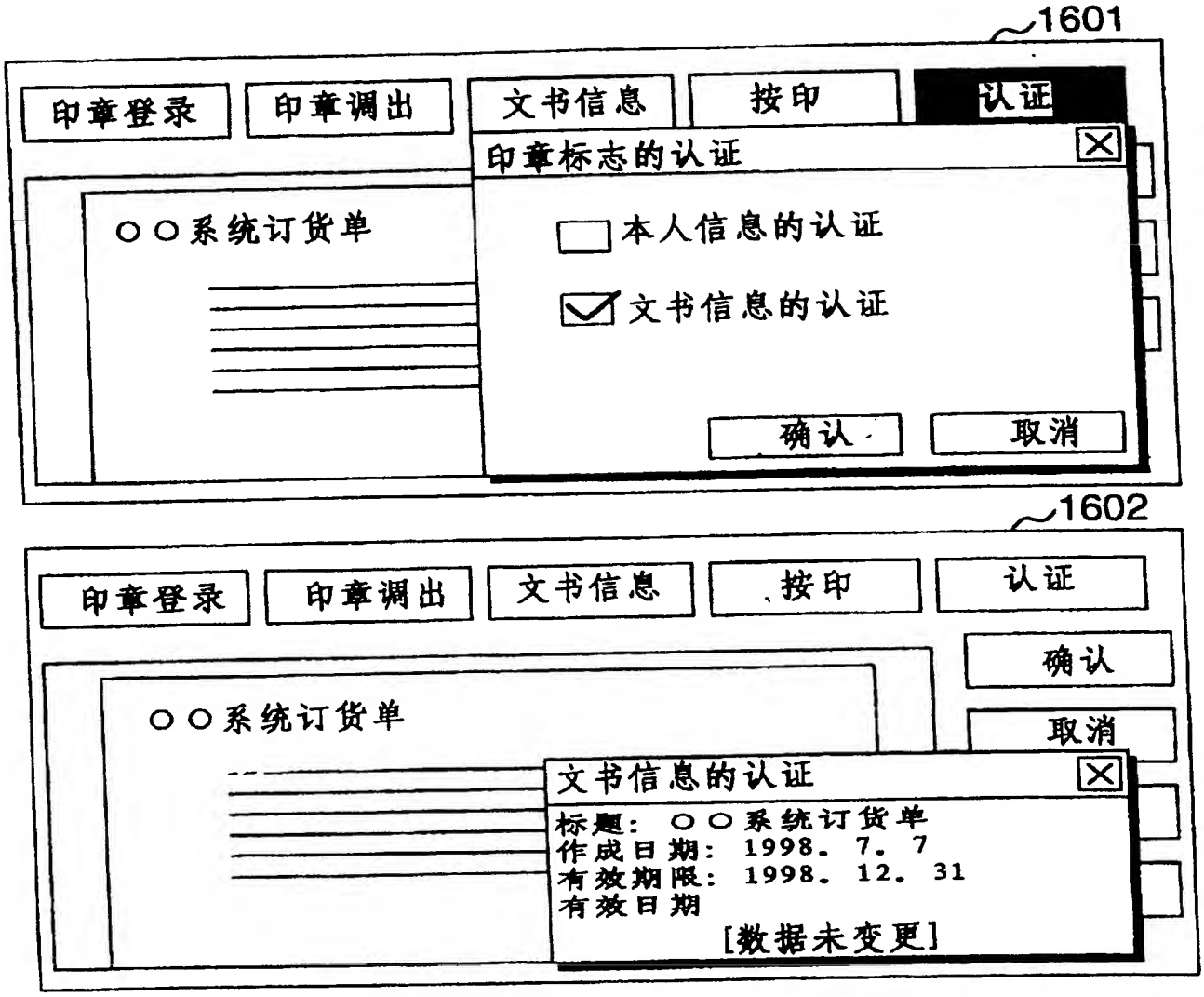

职员终端
111
识别单击的标志的文书认证项目
1501
从标志中抽出文书信息的译码键
1502
从标志中抽出文书信息
1503
将从标志中抽出的文书信息译码
1504
从文书中抽出文书的特征信息
1505
1506
将文书的特征信息进行比较对照
NG
1507
错误信息[设数据变更过了]
OK
1509
确认有效期限等
NG
将图章印痕变形为无效的图案等
1508
OK
确认并显示文书认识信息
1510
结束

图16


1601
印章登录
印章调出
文书信息
按印
认证
印章标志的认证
○○系统订货单
本人信息的认证
文书信息的认证
确认
取消
1602
印章登录
印章调出
文书信息
按印
认证
确认
取消
○○系统订货单
文书信息的认证
标题: ○○系统订货单
作成日期: 1998. 7. 7
有效期限: 1998. 12. 31
有效日期
[数据未变更]